CLAIMS

1. In a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a system for providing virus protection comprising:

a gateway coupled between the first network and the destination, which includes a firewall which receives the data packets and virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, tests the data packets, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested o contain a virus.

2. A system in accordance with claim 1, wherein:

the firewall classifies the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof.

3. A system in accordance with claim 2, wherein:

the virus scanning engine tests the data packets of the second type and forwards those data packets which are tested to not contain a virus to the destination.

4. A system in accordance with claim 2, wherein:

the data packets of the first type contain real time data.

5. A system in accordance with claim 3, wherein:

the data packets of the first type contain real time data.

6. A system in accordance with claim 1, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which, in response to the alert, stops reception of a data stream containing the data packets.

7. A system in accordance with claim 2, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

8. A system in accordance with claim 3, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

9. A system in accordance with claim 4, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

10. A system in accordance with claim 5, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

11. A system in accordance with claim 2 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

12. A system in accordance with claim 3 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

13. A system in accordance with claim 4 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

14. A system in accordance with claim 5 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

15. A system in accordance with claim 6 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

16. A system in accordance with claim 7 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

17. A system in accordance with claim 8 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

18. A system in accordance with claim 9 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

19. A system in accordance with claim 10 comprising:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

20. A system in accordance with claim 1 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

21. A system in accordance with claim 2 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

22. A system in accordance with claim 4 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

23. A system in accordance with claim 5 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

24. A system in accordance with claim 6 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

25. A system in accordance with claim 7 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

26. A system in accordance with claim 9 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

27. A system in accordance with claim 12 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

28. A system in accordance with claim 14 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

29. A system in accordance with claim 15 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

30. A system in accordance with claim 16 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

31. A system in accordance with claim 18 comprising:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

32. A system in accordance with claim 21 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

33. A system in accordance with claim 4 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

34. A system in accordance with claim 7 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

35. A system in accordance with claim 9 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

36. A system in accordance with claim 11 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

37. A system in accordance with claim 13 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

38. A system in accordance with claim 16 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

39. A system in accordance with claim 18 comprising:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

40. A system in accordance with claim 1, wherein:

the virus scanning engine, upon detection of a virus in the data packets, also alerts the destination that a virus has been detected.

41. A system in accordance with claim 1 wherein:

the destination is a local area network.

42. A system in accordance with claim 1 wherein:

the destination is a personal computer.

43. A system in accordance with claim 1, wherein:

the destination is a second network.

44. A system in accordance with claim 1, wherein:

the first network is a wide area network.

45. A system in accordance with claim 44, wherein:

the wide area network is the Internet.

46. A system in accordance with claim 1, wherein:

the first network is the Internet; and

the destination comprises an Internet service provider coupled to the gateway, a modem coupled to the Internet service provider and one of a local area or personal computer coupled to the modem.

47. A system in accordance with claim 1, wherein:

the virus scanning engine decodes the data packets during determination if the data packets contain a virus.

48. A system in accordance with claim 47, wherein:

the virus scanning engine functions as a proxy for a destination processor which receives the data packets.

49. In a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination which includes a firewall which receives the data packets and a virus scanning engine, a method comprising:

receiving the data packets at the firewall;

transmitting the received data packets from the firewall to the virus scanning engine;

testing the data packets with the virus scanning engine; and

transmitting from the virus scanning engine any data packets which are tested by the virus scanning engine to not contain any virus to the destination and the discarding any data packets which are tested to contain a virus.

50. A computer program stored on a storage medium for use in a virus scanning engine in a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a firewall which receives the data packets and the virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus, the computer program when executed causing the virus scanning engine to execute at least one step of:

testing the data packets for the presence of a virus.

51. A computer program in accordance with claim 50, wherein the firewall classifies the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof, wherein:

the computer program when executed causes the virus scanning engine to test the data packets of the second type and causes the virus scanning engine to forward those data packets which are tested to not contain a virus to the destination.

52. A computer program in accordance with claim 50 wherein:

the computer program when executed causes the virus scanning engine to forward any data packets which are tested to not contain a virus to the destination and causes the virus scanning engine to discard any data packets which contain a virus.

53. A computer program in accordance with claim 51, wherein:

the data packets of the first type contain real time data.

54. A computer program in accordance with claim 50, wherein:

the computer program when executed causes the virus scanning engine, when a virus is detected, to alert the firewall that a virus has been detected which, in response to the alert, stops reception of a data stream containing the data packets.

55. A computer program in accordance with claim 50, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules, a packet classification database is coupled to the firewall which provides information to the firewall which defines the first and second types of data packets and a virus detection database is coupled to the virus scanning engine, wherein:

the computer program controlling the testing of the data packets of the second type by the virus scanning engine is provided to the virus scanning engine from the virus detection database.